REMARKS

This reply is responsive to the Office Action mailed on April 27, 2005. Claims 1-9 are pending in the application. Reconsideration in light of the following remarks is respectfully requested.

I. Specification

The Specification was objected to by the Examiner due to certain informalities. The first paragraph of the Specification is amended by the Response to include appropriate application numbers and filing dates as requested by the Examiner. Withdrawal of the objection is respectfully requested.

II. Rejection under 35 U.S.C. § 103

A. Claims 1, 2, and 7

Claims 1, 2, and 7 stand rejected under 35 U.S.C. § 103, as being obvious over Tanaka (U.S. Patent No. 5,029,208, issued July 2, 1991) in view of Doonan et al. (U.S. Patent No. 6,807,277, issued October 19, 2004 (Doonan). Applicants respectfully disagree.

Tanaka discloses a "cipher-key distribution system used in a one-way communication from a first party to a second party. The cipher-key distribution system is composed of a first subsystem, a second subsystem, and a common file which stores information publically accessible by the first and second subsystems. The first subsystem generates a cipher-key based on a constant, receiving party identifying information, a random number, and public information from the common file. The first subsystem also generates a key distributing code based on a constant, a random number and a first secret information and transfers the key distributing code to a second subsystem. The second subsystem receives the key distributing code and information for identifying the first party and generates a second cipher-key identical to the cipher-key generated by the first subsystem. The second cipher-key is created from the information for identifying the first party, a second secret information, and the key distributing code. The first subsystem, instead of generating and transmitting a key distributing code, may simply transmit information for identifying the first communicating party to the second subsystem." (Tanaka, Abstract)

Doonan discloses a "method and system for electronic messaging in which a sender of an electronic message receives a return receipt, without having to send the message contents to a third party. The sender contacts a server to obtain an encryption key to encrypt the message. The server returns an encryption key along with key retrieval information to the sender. The key retrieval information can be used to obtain from the server the decryption key corresponding to the returned encryption key. The sender encrypts the message using the encryption key and sends the message, along with the key retrieval information, to the recipient. The recipient sends the key retrieval information to the server to retrieve the corresponding decryption key. The recipient then decrypts the encrypted message received from the sender using the decryption key. When the recipient sends a request to obtain the decryption key, the server notifies the sender when the key has been successfully retrieved. The fact that the decryption key was retrieved by the recipient indicates to the sender that the recipient received the message." (Doonan, Abstract)

The Examiner's attention is directed to the fact that Tanaka and Doonan, either singly, or in any permissible combination fail to disclose that "upon initialization, the client provides its public key, authenticated with the provisioning key for forwarding to the key distribution center" as recited in independent claims 1 and 7. Specifically independent claims 1 and 7 recite:

1. A provisioning system that secures delivery of a client public key, the provisioning system comprising:
a client to be registered;
a provisioning server for registering the client and assigning it a unique user ID (identification);
a key distribution center for generating a provisioning key associated with the user ID, the provisioning key being forwarded to the provisioning server;
the provisioning server generating configuration parameters for initializing the client, the provisioning key being included in the configuration parameters; and
upon initialization, the client provides its public key, authenticated with the provisioning key for forwarding to the key distribution center. (emphasis added)

7. A method for initially establishing trust between a KDC (Key Distribution Center) and a client having a uniquely identifiable user ID (identification) that was assigned by the provisioning server, the method comprising:
generating, by the KDC, a provisioning key associated with the user ID, the provisioning key being forwarded to the provisioning server;
forwarding the provisioning key to a provisioning server for registering the client;
generating, by the provisioning server, configuration parameters for initializing the client;
forwarding to the client, the provisioning key and the configuration parameters for initializing the client; and
upon initialization, the client provides its public key, authenticated with the provisioning key for forwarding to the key distribution center. (emphasis added)

The present invention discloses a provisioning system that secures delivery of a client's public key to a KDC (Key Distribution Center). During registration, the provisioning system allows the initial establishment of trust between the client and the KDC server so the client can receive real-time data streams from a content provider. The

KDC generates a provisioning key associated with the client ID, after which the provisioning key is forwarded to a provisioning server. Configuration parameters for initializing the client are generated by the provisioning server, the provisioning key being included in the configuration parameters. These parameters are used by the client for initialization. In one embodiment, upon initialization, the client generates a private/public key pair of which the public key is forwarded to the KDC. When forwarded, the public key is authenticated with the provisioning key previously received by the client.

In contrast, Tanaka fails to teach the forwarding of an authenticated public key to a key distribution center. In addition, the Examiner concedes that Tanaka fails to teach the use of a provisionary or intermediate server. Tanaka teaches that its public information is stored in a common file and is not forwarded to its key distribution center. In fact, Tanaka fails to teach the forwarding of any information to the key distribution center. (See Tanaka; Fig. 1; and Abstract, lines 9-22)

Doonan, likewise, also fails to teach the forwarding of an authenticated public key to a key distribution center. Doonan teaches the sending of an encryption key and key retrieval information from a key server to a sender who intends to send an encrypted message to a recipient. The encryption key is used to encrypt a message from the sender to the recipient and the encrypted message is sent to the recipient along with the key retrieval information. In fact, Doonan fails to teach the forwarding of any information, besides an encryption key request (from the sender) or a key retrieval request (from the recipient), to the key server. Instead, Doonan teaches that a public key certificate is **generated by** the key server. (See Doonan, col. 4, lines 36-43; "a credential is generated according to the authentication policy of the key server. Included among these credentials may be a userid and password selected by the key server or by the user, or a public key certificate issued by the key server.") Clearly, Doonan teaches away from the forwarding of an authenticated public key to a key distribution center.

In addition, Applicants submit that there is no motivation to combine Tanaka with Doonan and that the systems of Tanaka and Doonan are incompatible. The key distribution center of Tanaka **only** generates information that is used by a first subsystem to cipher a message to a second subsystem. The second subsystem does **not** receive a cipher key from the key distribution center. Instead, the second subsystem uses ID information from the first subsystem in order to generate a cipher key. In contrast, Doonan teaches that the sender receives an encryption key from the key server and uses that encryption key to encrypt a message to a recipient. The encrypted message is sent along with key retrieval information to the recipient. The recipient then uses the key retrieval information to generate a key retrieval request. In response to the key retrieval request, the key server forwards a decryption key to the recipient. Doonan clearly uses a key server to distribute encryption/decryption keys. Thus Tanaka is clearly incompatible with Doonan since Tanaka does not teach using a key server or key distribution center to generate and/or send encryption and decryption keys.

Therefore, Applicants submit that independent claims 1 and 7 are patentable over Tanaka and Doonan. Claim 2 is patentable at least by virtue of depending from its respective base claim. Applicants respectfully request withdrawal of the rejection.

B. Claims 3-5, 8, and 9

Claims 3-5, 8, and 9 stand rejected under 35 U.S.C. § 103 as being unpatentable over Tanaka and Doonan in view of Kohl (Kohl, J., "The Kerberos Network Authentication Service", RFC 1510, September 1993, pp. 1-7, 16-35). Applicants respectfully disagree.

The Examiner concedes that Tanaka and Doonan fail to disclose the use of tickets. Kohl was cited in order to cure the Examiner's perceived deficiency of Tanaka and Doonan.

Kohl discloses an overview and specification of Version 5 of the protocol for the Kerberos network authentication system. Kerberos provides a means of verifying the identities of principals, (e.g., a workstation user or a network server) on an open (unprotected) network. This is accomplished without relying on authentication by the host operating system, without basing trust on host addresses, without requiring physical security of all the hosts on the network, and under the assumption that packets traveling along the network can be read, modified, and inserted at will.

As argued above in Section II. A., Tanaka and Doonan, either singly, or in any permissible combination fail to disclose that "upon initialization, the client provides its public key, authenticated with the provisioning key for forwarding to the key distribution center" as recited in independent claims 1 and 7. Kohl fails to cure the deficiencies of Tanaka and Doonan as noted in Section II. A. As such, Applicants submit that claims 3-5, 8, and 9 are patentable at least by virtue of depending from their respective base claim. Therefore, Applicants respectfully request withdrawal of the rejection.

C. Claim 6

Claim 6 stands rejected under 35 U.S.C. § 103 as being unpatentable over Tanaka and Doonan in view of FOLDOC (FOLDOC, "Internet Address", December 1994, p. 1). Applicants respectfully disagree.

The Examiner concedes that Tanaka and Doonan fail to disclose the client provides a host identifier that uniquely identifies a computer on which the client application is running. FOLDOC was cited in order to cure the Examiner's perceived deficiency of Tanaka and Doonan.

FOLDOC discloses the 32-bit host address defined by the Internet Protocol in STD 5, RFC 791. A hosts's Internet address is sometimes related to its Ethernet address. The Internet address is usually expressed in dot notation, e.g. 128.121.4.5. The address can be split into a network number (or network address) and a host number unique to each host on the network and sometimes also a subnet address. The way the address is split depends on its "class", A, B or C as determined by the high address bits: Class A - high bit 0, 7-bit network number, 24-bit host number. n1.a.a.a 0 <= n1 <= 127; Class B - high 2 bits 10, 14-bit network number, 16-bit host number. n1.n2.a.a 128 <= n1 <= 191; Class C - high 3 bits 110, 21-bit network number, 8-bit host number. n1.n2.n3.a 192 <= n1 <= 223. The Internet address must be translated into an Ethernet address by either ARP or constant mapping.

As argued above in Section II. A., Tanaka and Doonan, either singly, or in any permissible combination fail to disclose that "upon initialization, the client provides its public key, authenticated with the provisioning key for forwarding to the key distribution center" as recited in independent claim 1. FOLDOC fails to cure the deficiencies of Tanaka and Doonan as noted in Section II. A. As such, Applicants submit that claim 6 is patentable at least by virtue of depending from its respective base claim. Therefore, Applicants respectfully request withdrawal of the rejection.

Conclusion

Having fully responded to the Office action, the application is believed to be in condition for allowance. Should any issues arise that prevent early allowançe of the above application, the examiner is invited contact the undersigned to resolve such issues.

To the extent an extension of time is needed for consideration of this response, Applicant hereby request such extension and, the Commissioner is hereby authorized to charge deposit account number 502117 for any fees associated therewith.

Date: 8/4/2005

Respectfully submitted,

By:
Thomas Bethea, Jr.
Reg. No.: 53,987

Motorola Connected Home Solutions
101 Tournament Drive
Horsham, PA 19044
(215) 323-1850